after decrypting the application key, erasing the operation key temporarily saved within a second volatile memory in the first unit.

A2 cncld.

18. (Once Amended) A method according to claim 2, further comprising:

sending the random information, information pertaining to an application key and information specific to the second unit to the first unit by means of a first single command.

19. (Once Amended) A method according to claim 20, further comprising:

sending the encrypted application key and the information pertaining to an application key to the second unit by means of a single second command.

Remarks

The amendments have been made in order to comply with the formal requirements of the USPTO. No new matter was introduced by such amendments, and no amendments were made for reasons relating to patentability. Favorable consideration of this application is respectfully requested.

Please apply any charges not covered, or any credits, to Deposit Account 500-591 (Reference No. 9669.004001).

Respectfully submitted,

Date: 2/8/01

Jonathan P. Osha, Reg. No. 33,986
Rosenthal & Osha L.L.P.
700 Louisiana, Suite 4550
Houston, TX 77002

Telephone: (713) 228-8600
Facsimile: (713) 228-8778

18622_1.DOC

APPENDIX A – MARKED-UP VERSION OF THE CLAIMS

Newly added matter has been indicated by underline, while matter to be appears in brackets and boldface.

2. (Once Amended) A method according to claim **[1]** 20, **[characterized in that it further comprises an additional step of]** further comprising:

[-] sending information specific to the second unit **[(EI)]** to the first unit **[(AS)]** before computing the application key **[(T1)]** in the first unit **[(AS)]**.

3. (Once Amended) A method according to **[claims 1 or 2]** claim 20, **[characterized in that it further comprises an additional step of]** further comprising:

[-] sending a random number provided by the second unit **[(EI)]** to the first unit **[(AS)]**, before encrypting the application key **[(TA)]** in the first unit **[(AS)]**.

4. (Once Amended) A method **[according to any of the preceding claims, characterized in that it further comprises an additional step of]** according to claim 20, further comprising:

[-] sending information pertaining to an application key **[(TA)]** to the first unit **[(AS)]**, before encrypting the application key **[(TA)]** within said first unit **[(AS)]**.

5. (Once Amended) A method according to claim 4, **[characterized in that it further comprises an additional step of]** further comprising:

[-] choosing the application key **[(TA)]** to be encrypted based on said information.

6. (Once Amended) A method **[according to any of the preceding claims, characterized in that]** according to claim 20, wherein said encryption of an application key **[(TA)]** intended for a second unit **[(EI)]** is unique.

7. (Once Amended) A method **[according to any of the preceding claims, characterized in that it further comprises and additional step of]** according to claim 20, further comprising:

[-] verifying integrity of the data **[(DATA)]** includes the encrypted application key **[(TA)]**.

8. (Once Amended) A method **[according to any of the preceding claims, characterized in that it further comprises an additional step of]** according to claim 20, further comprising:

[-] sending information pertaining to an application key **[(TA)]** to the second unit **[(EI)]**, before decrypting the encrypted application key **[(TA)]** within said second unit **[(EI)]** of said set **[(S)]**.

9. (Once Amended) A method **[according to any of the preceding claims, characterized in that it further comprises an additional step of]** according to claim 20, further comprising:

[-] storing within the second unit **[(EI)]**, after decrypting the encrypted application key **[(TA)]**, said key **[(TA)]** within said second unit **[(EI)]**.

10. (Once Amended) A method according to claim 9, **[characterized in that]** wherein storing of the application key **[(TA)]** within the second unit **[(EI)]** is done based on information pertaining to an application key **[(TA)]**.

11. (Once Amended) A method **[according to any of the preceding claims, characterized in that it further comprises an addition step of]** according to claim 20, further comprising:

[-] verifying that the application key **[(TA)]** is authentic.

12. (Once Amended) A method **[according to any of the preceding claims, characterized in that]** according to claim 20, wherein the first security unit **[(AS) is]** comprises a smart card.

13. (Once Amended) A method **[according to any of the preceding claims, characterized in that]** according to claim 20, wherein the memory **[(M) is]** comprises a rewritable memory.

14. (Once Amended) A method **[according to any of the preceding claims, characterized in that]** according to claim 20, wherein a second unit **[(EI)]** comprises several application keys **[(TA)]**.

15. (Once Amended) A method **[according to any of the preceding claims, characterized in that]** according to claim 20, wherein the first unit **[(AS)]** comprises several application keys **[(TA)]**.

16. (Once Amended) A method **[according to any of the preceding claims, characterized in that it further comprises an additional step of]** according to claim 20, further comprising:

[-] after encrypting the application key **[(TA)]**, erasing the operation key **[(T1)]** temporarily saved within the second volatile memory of the first unit **[(AS)]**.

17. (Once Amended) A method **[according to any of the preceding claims, characterized in that it further comprises an additional step of]** according to claim 20, further comprising:

[-] after decrypting the application key **[(TA)]**, erasing the operation key **[(T1)]** temporarily saved within a second volatile memory **[(M2)]** in the first unit **[(EI)]**.

18. (Once Amended) A method **[according to preceding claims 2 to 4, characterized in that it further comprises an additional step of]** according to claim 2, further comprising:

[-] sending the random information, information **[(REF1)]** pertaining to an application key **[(TA)]** and information **[(SN)]** specific to the second unit **[(EI)]** to the first unit **[(AS)]** by means of a first single command **[(EXPORTKEY)]**.

19. (Once Amended) A method [according to preceding claims 1 and 2, characterized in that it further comprises the additional steps of] according to claim 20, further comprising:

[-] sending the encrypted application key [(TA)] and the information [(REF2)] pertaining to an application key [(TA)] to the second unit [(EI)] by means of a single second command [(IMPORTKEY)].